Electronic Version
Stylesheet Version v1.1.1

Geometry-Based Symmetric Cryptosystem Method

Abstract

A method of communicating information between users of a communication system includes the following steps of: generating a module V over a ring R; generating an outer component P of encryption key that includes sequence (p_1, p_2, ..., p_k) where each member p_j of the sequence belongs to the set {1, 2, ..., m} (the length k of the sequence is arbitrary and thus repetitions are allowed in the sequence); generating an inner component Q of encryption key that includes elements v_1, v_2, ... v_m of V and automorphisms g_1, g_2, ... , g_m of V; generating the encryption key K = (P; Q), where P is the outer component and Q is the inner component; generating an encryption automorphism T_e of V based on the encryption key K, where T_e includes a composition of certain automorphisms T_1, T_2, ... , T_m of the module V which composition is performed in the order prescribed by P; generating an encrypted message element E as a function of a message element M in V and of the encryption automorphism T_e; transmitting the encrypted message element E along with the outer component P

from one user to another; generating the outer component P' of the decryption key that includes sequence (p_k, p_{k-1}, ... , p_1), i.e., the sequence reversed of that involved in producing the outer component P of the encryption key; generating the decryption key K' = (P'; Q'), where P' is the outer component of the decryption key and Q' is the inner component of the decryption key which is equal to the inner component Q of the encryption key; generating a decryption automorphism T_d of V based on the decryption key K', where T_d includes a composition of the automorphisms T_1, T_2, ..., T_m, which composition is performed in the order prescribed by P', e.g., T_d is the inverse automorphism of T_e; determining the message element M as a function of the encrypted message element E and of the decryption automorphism T_d, where the function is the same as that one used in generation of E (that is, the decryption method is symmetric to encryption: the decryption proceeds as the encryption, but with replacement of the outer component P with the outer component P').